

Understanding Cyber Defense

A Systems Architecture Approach



Tom McDermott

Director of Research
Georgia Tech Research Institute
tom.mcdermott@gtri.gatech.edu

Todd Moore

Manager, San Diego Office
Georgia Tech Research Institute
todd.moore@gtri.gatech.edu

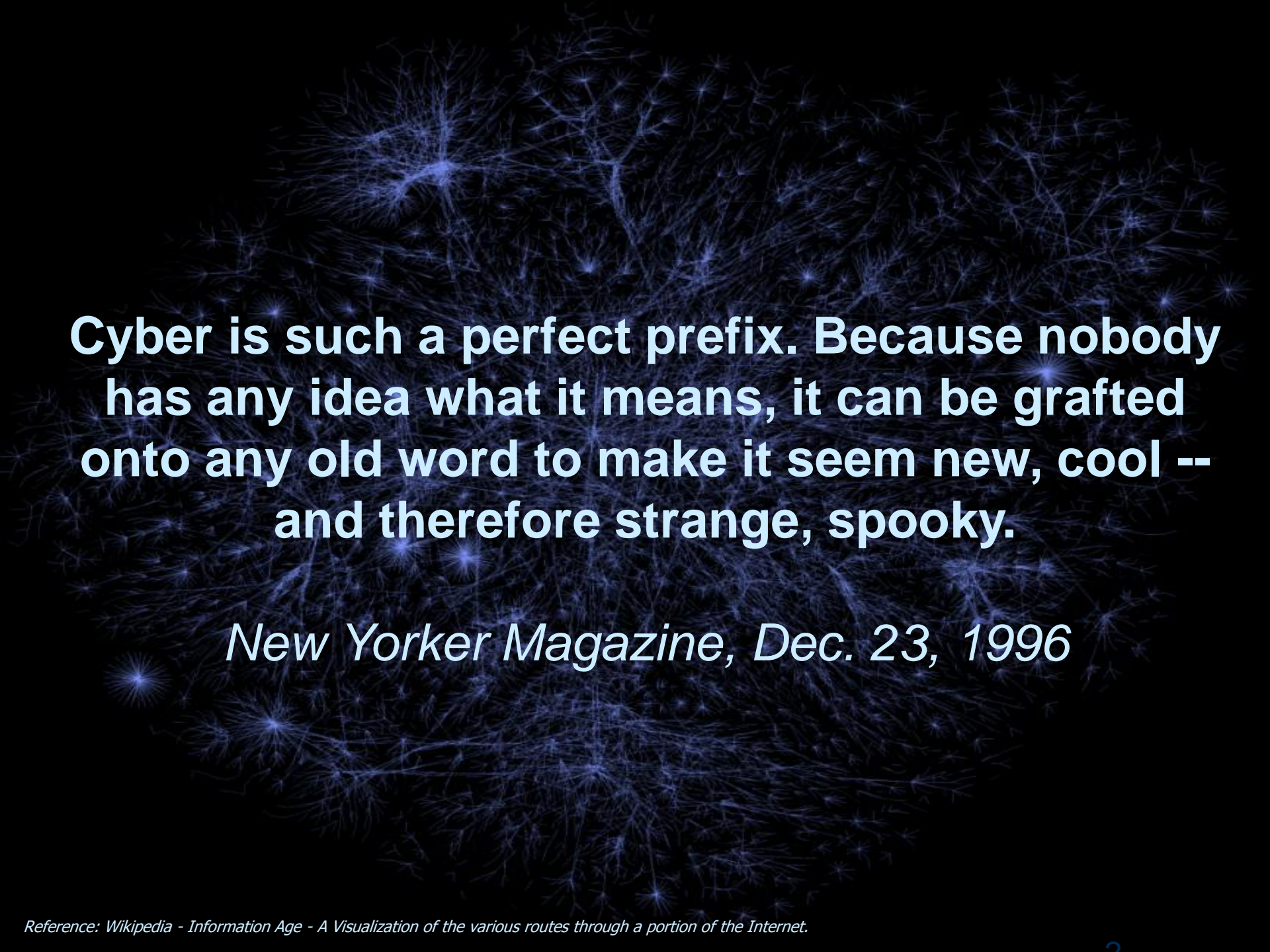
Jeff Moulton

Director, Program Development
Georgia Tech Research Institute
jeff.moulton@gtri.gatech.edu

Josh Davis

Senior Research Engineer
Georgia Tech Research Institute
Josh.davis@gtri.gatech.edu





Cyber is such a perfect prefix. Because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool -- and therefore strange, spooky.

New Yorker Magazine, Dec. 23, 1996

What is Cyber Security?

Computer security - protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

Network security - consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources

Information security - protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Cybersecurity - measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Current State, Unattributed Quotes

- ◆ “The state of cyber security today is a complete failure...If you haven’t been hacked you have nothing of interest to steal”
- ◆ “fundamental trust models in cyberspace are broken; there is no technology out there today that reflects trust; 100 years from now we will realize we were in a lawless state”
- ◆ “why do we lack systems understanding, holistic design principles, risk management, and training in our enterprise systems?”
- ◆ “we are our worst enemies...the problem is too huge...we cannot conceptualize it, cannot worry about it”
- ◆ “it’s going to take a ‘BP oil spill of data’ event to wake us up”

Current State is Rapidly Evolving & Expanding

- ◆ Hacker (1960's)
 - A person who enjoys exploring the details of programmable systems and stretching their capabilities
- ◆ “WarGames” (1983)
 - A young hacker starts the countdown to World War 3.
- ◆ Computer Viruses (1980's)
 - Tool era - Self-replication & connectivity
- ◆ Hacktivism (1990's)
 - WANK Worm ... to Anonymous & Lulz
- ◆ Cyber Criminals (2000's)
 - Financial theft, illicit trade
- ◆ Cyber Espionage (last decade)
 - Characterized by persistence
- ◆ Cyber Kinetic Attacks (emerging)
 - Primarily nation-state based, target physical systems



Current State is Rapidly Evolving

- ◆ Remarkable change in attack motivation from our IT Systems to our Enterprises
- ◆ Around 2005, saw attacks shift from individual IT systems to commercial enterprises
 - Unprecedented transfer of wealth, not just IP but also enterprise strategies
 - Organized crime and nation-state involvement
- ◆ Key threat shift: preparation and patience
 - Not hacking – normal IT tradecraft used, but the technology is mainstream
 - Espionage: reconnaissance, exfiltration, exploitation, profit
- ◆ New paradigms – “we have no idea what’s out there”

This is a Systems Problem

- ◆ No longer just an information technology issue
- ◆ Need to move from a vulnerability-centric model to a threat-centric model
- ◆ Need to move from a tool-centric perspective to a value-centric perspective
- ◆ Organizations must have a strategic cyber defense plan that drives their business approach
- ◆ The strategic plan must be threat-driven with targeted protection practices
- ◆ Protection practices center around information, not IT

This is a Complex Adaptive System

“everyone has a plan until they are punched in the face” (Mike Tyson)

- ◆ Threats and enterprise technologies are rapidly changing
- ◆ Cyber protection frameworks are dynamic and require constant reassessment

“our dependency is scary”

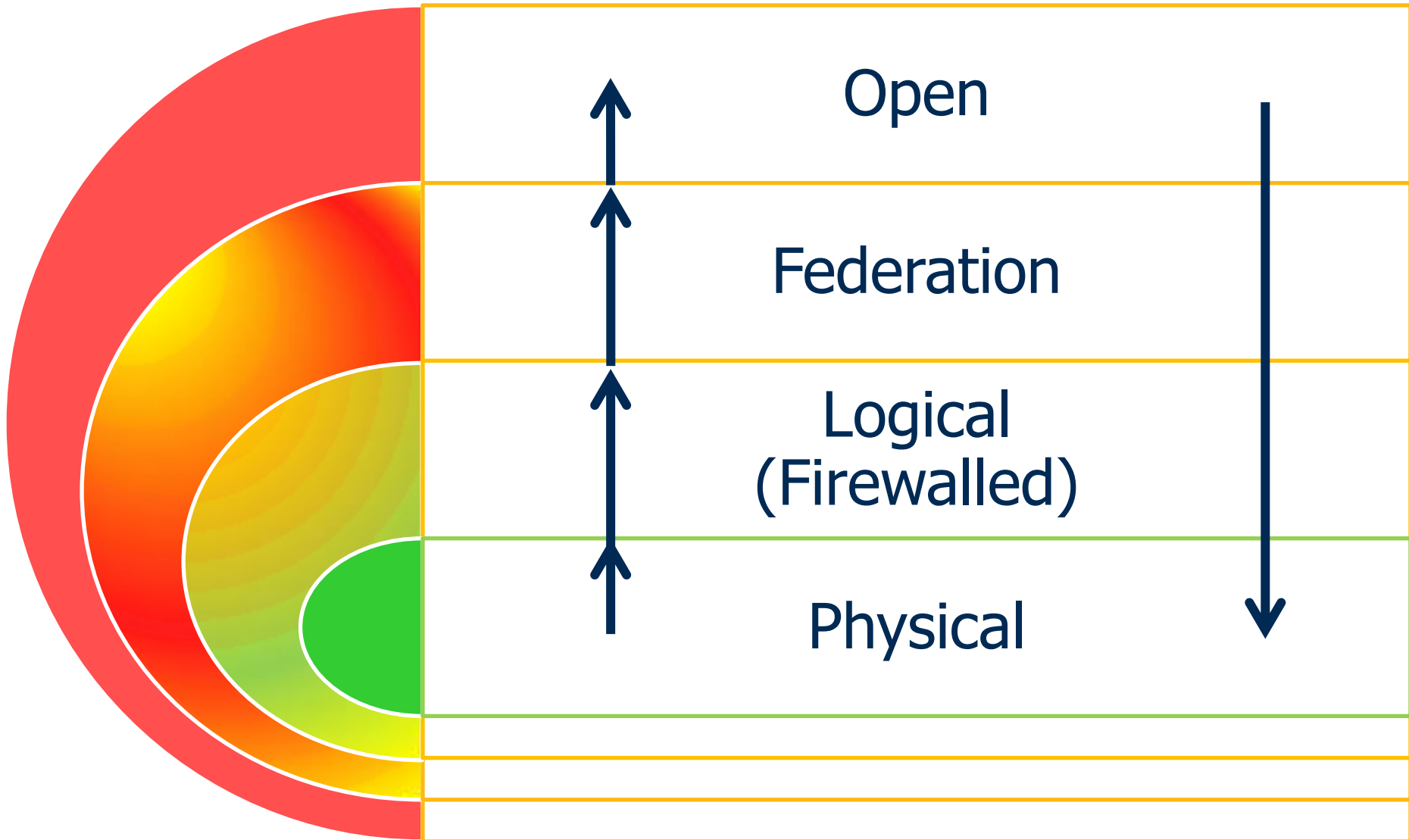
“protection is futile, resilience is the key”

- ◆ IT Systems, business practices, and social systems are completely intertwined
- ◆ Do you understand how complex this is?

Systems Architecture Assessment

1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?

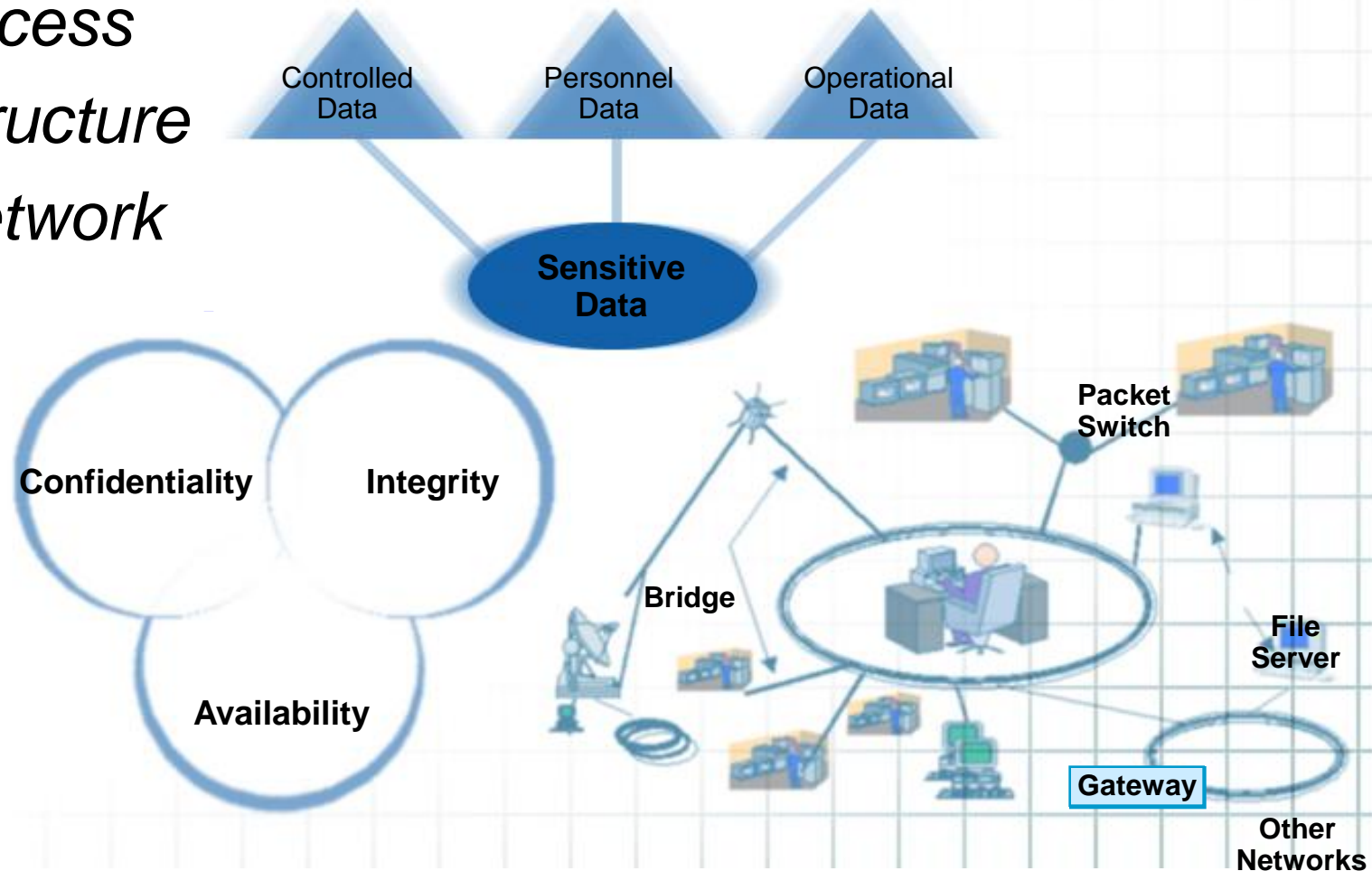
Today's Information Access View



When Information Becomes Digital Data

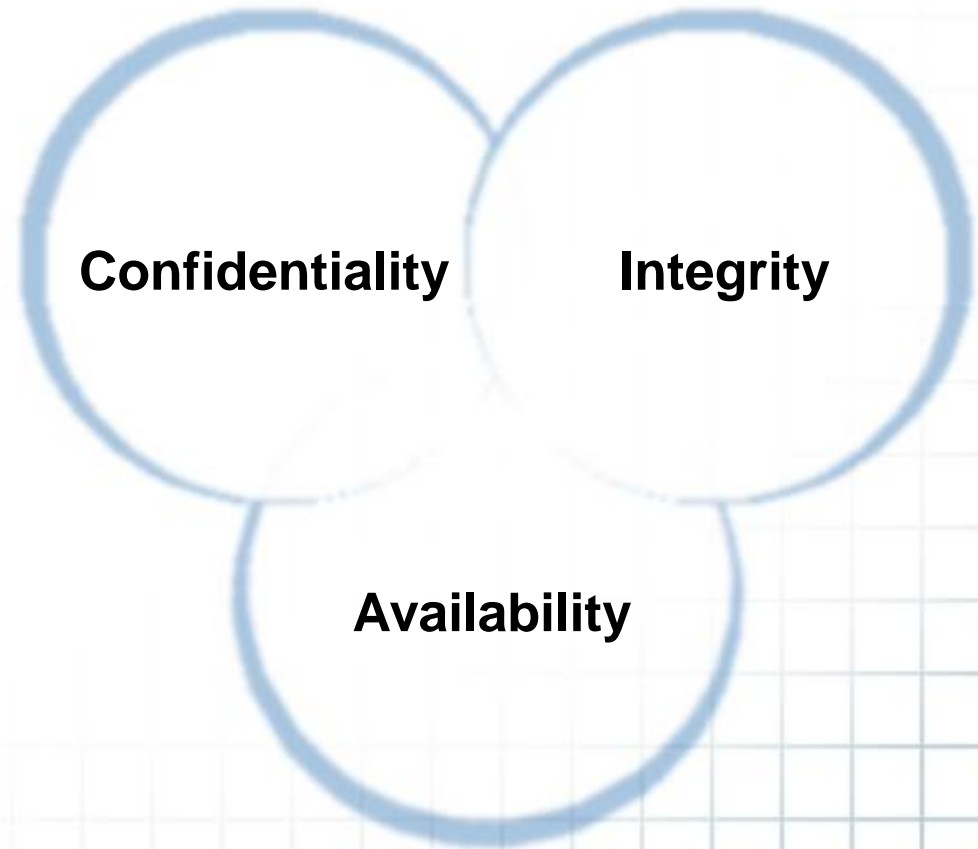
Concerned with:

- ◆ Data Access
- ◆ Data Structure
- ◆ Data Network



C-I-A Concerns: Access to the Data

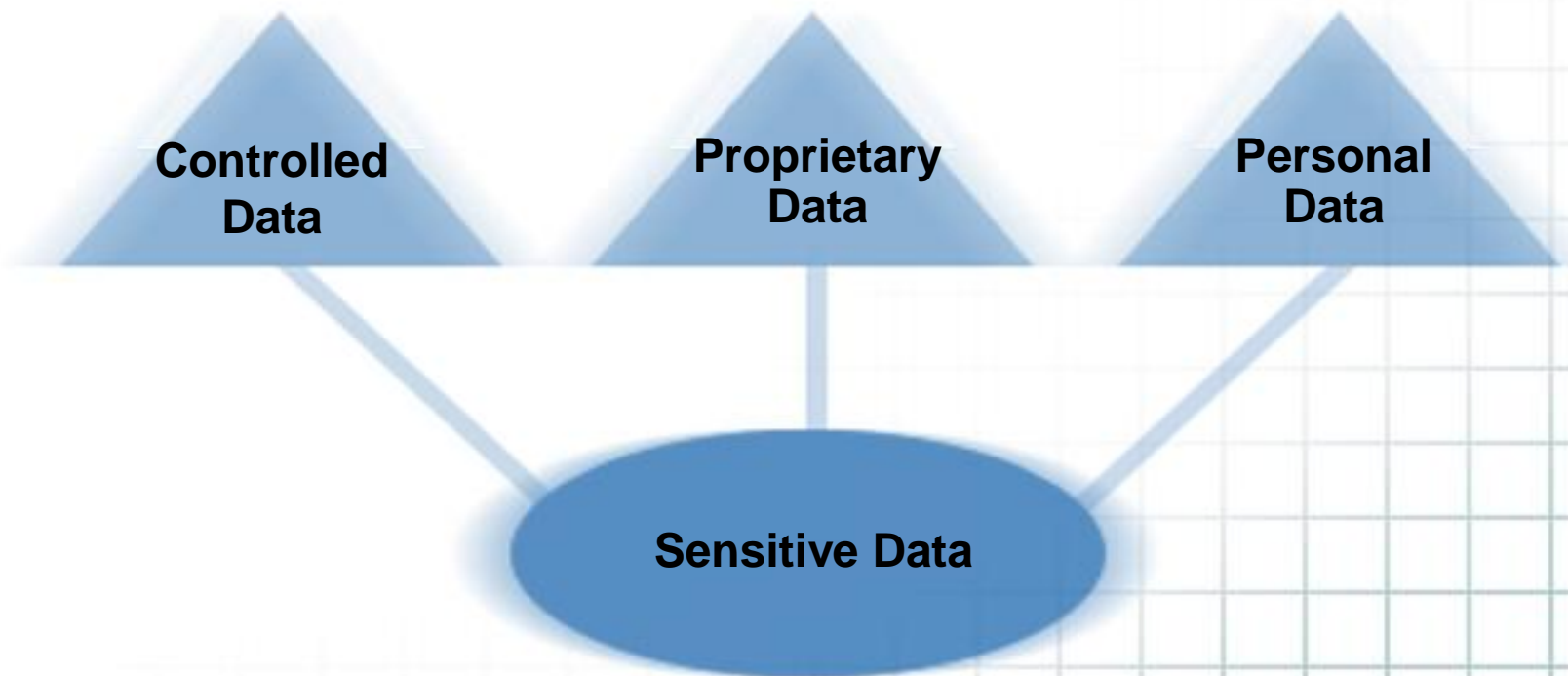
- ◆ Confidentiality
 - No disclosure
 - Only those who need to see data should see it
- ◆ Integrity
 - No alteration
 - Only those allowed to alter data can modify it
- ◆ Availability
 - No interruption
 - Everyone who needs to access data can access it



Data/Database Concerns

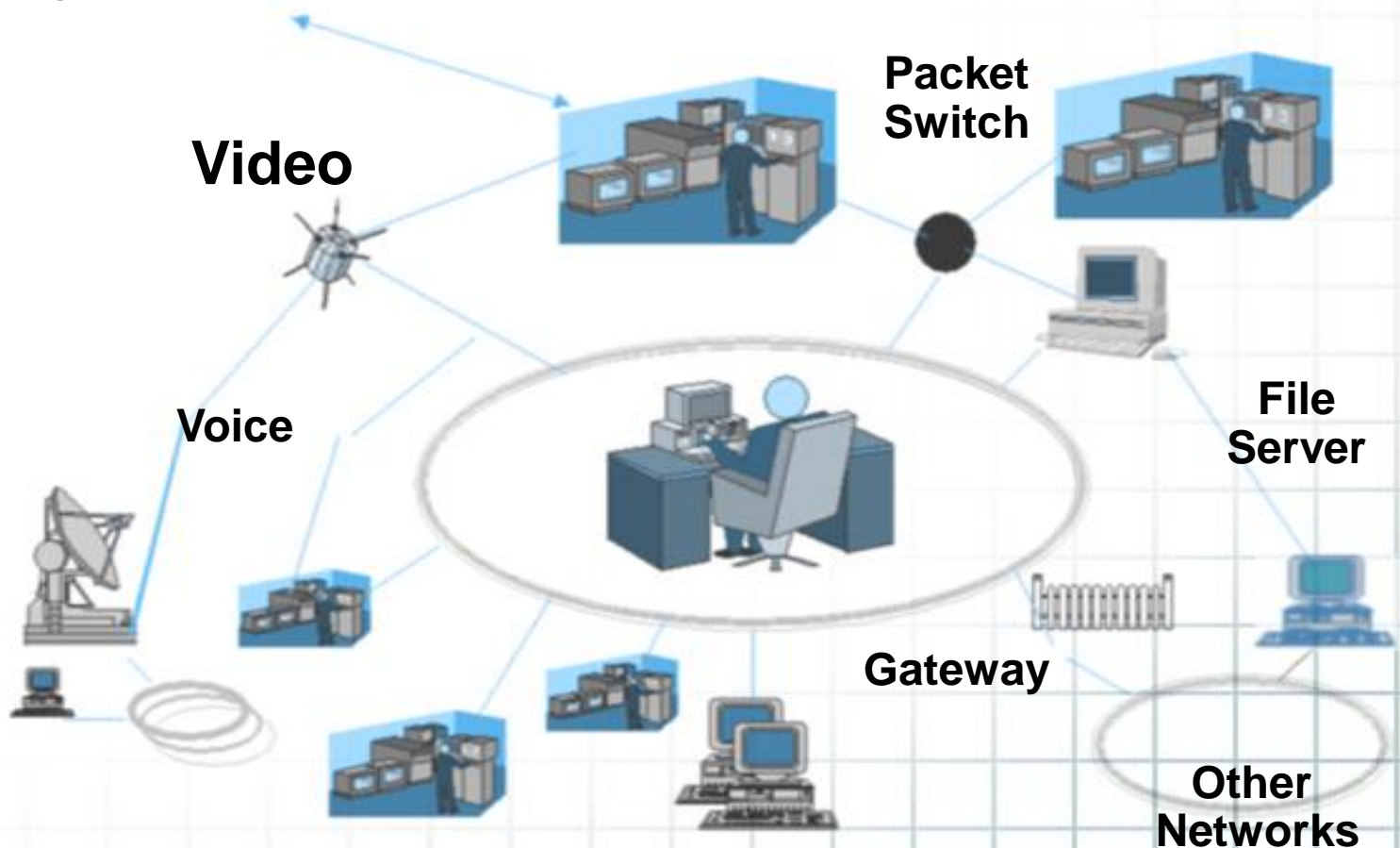
Data Aggregation, Data Inference & Polyinstantiation

- ◆ “The protection of the database and data elements against unauthorized access, either intentional or accidental”

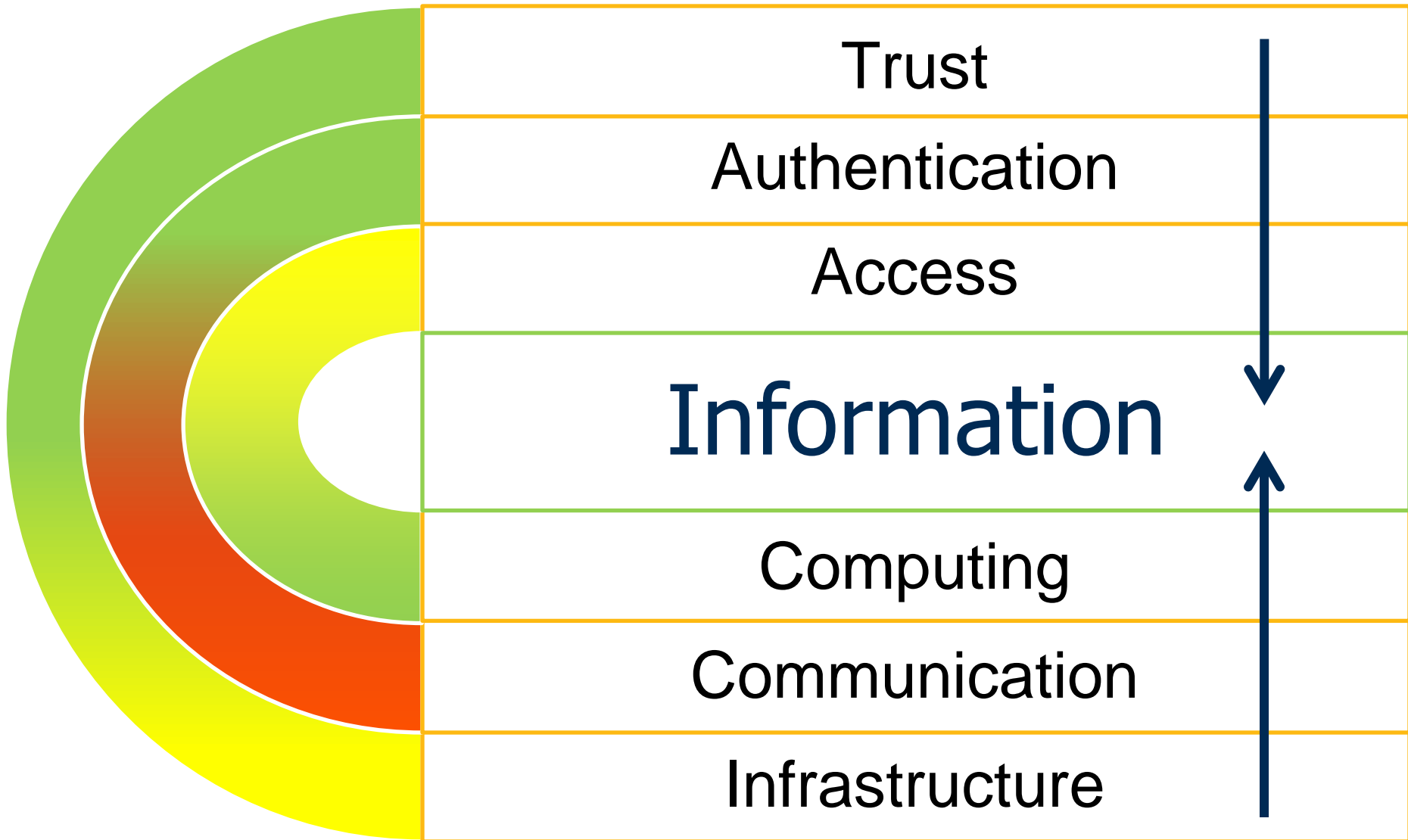


Network Concerns - Inter-Connectivity

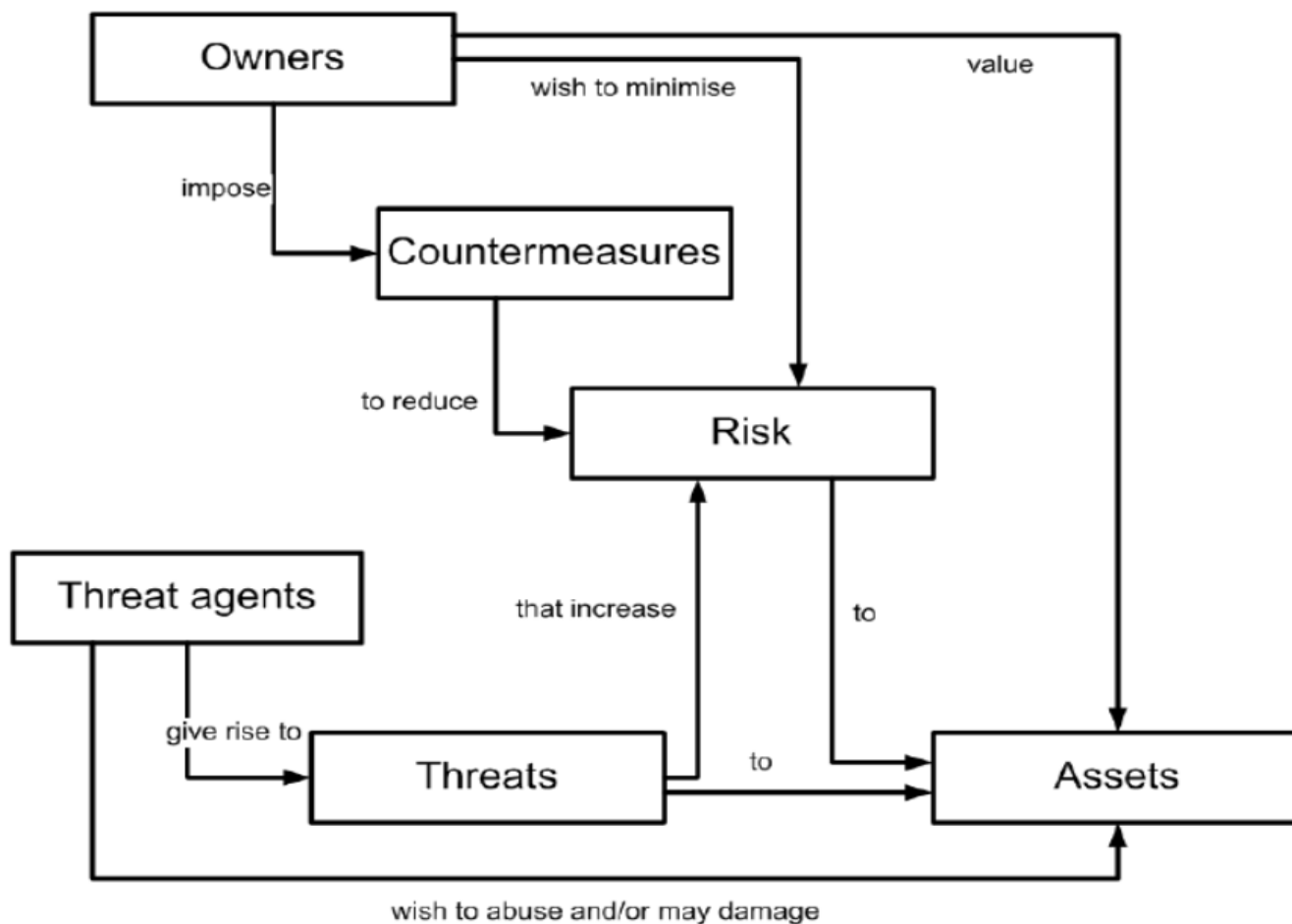
- ◆ Hardware
- ◆ Software
- ◆ Data



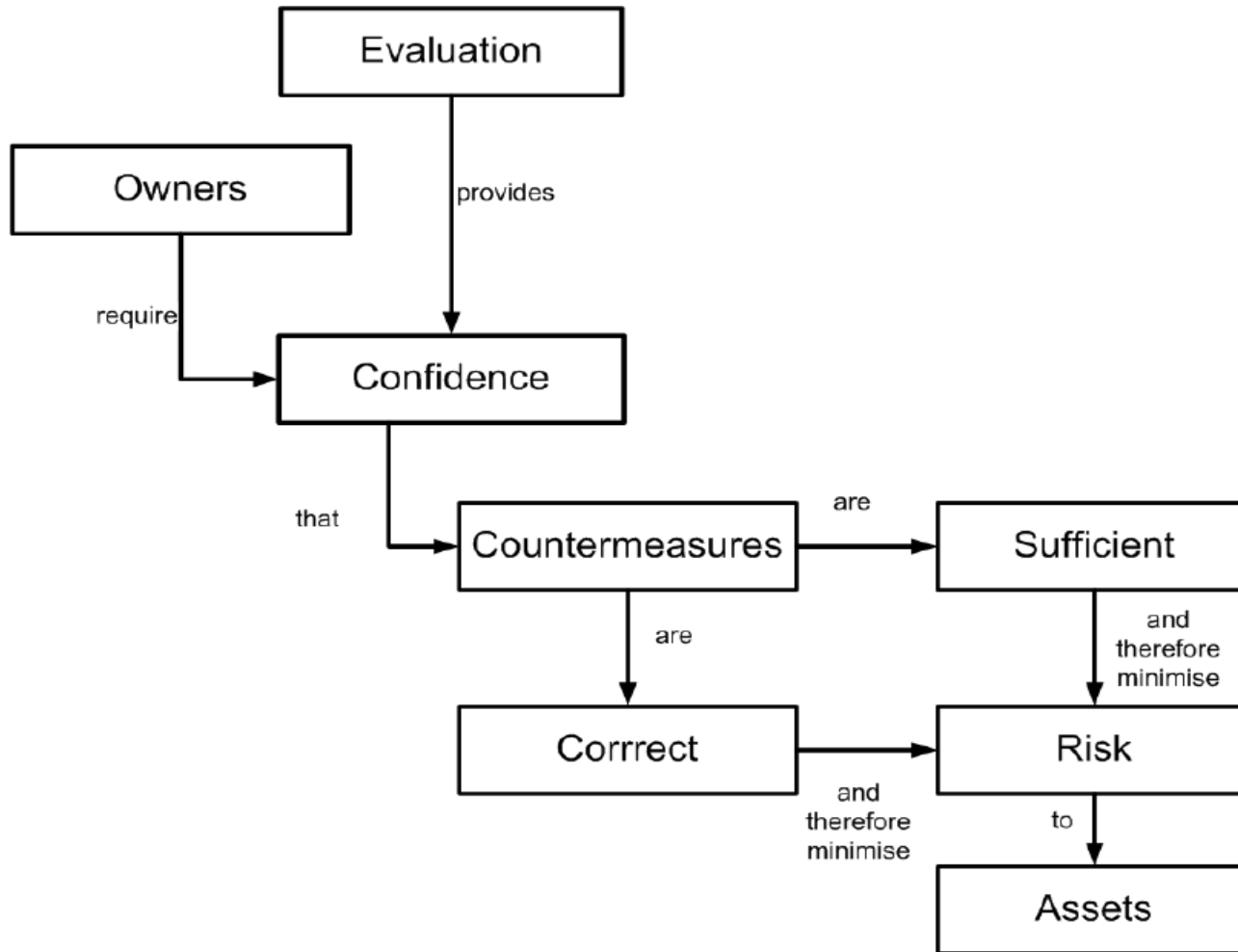
IT Systems have Logical Access Layers



IA Policy Model is Risk and Threat-Based



IA Policy not Useful Without Evaluation



Common Criteria for Information Technology Security Evaluation
<http://www.commoncriteriaportal.org/>

Business Drivers: Starts with the Information

1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?

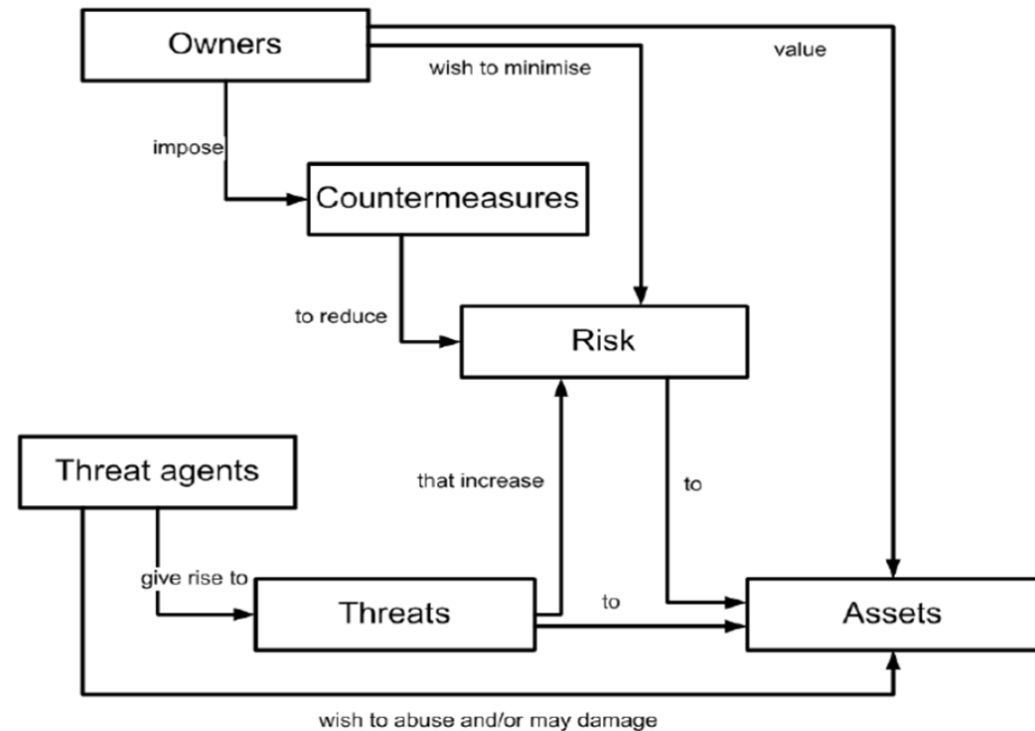
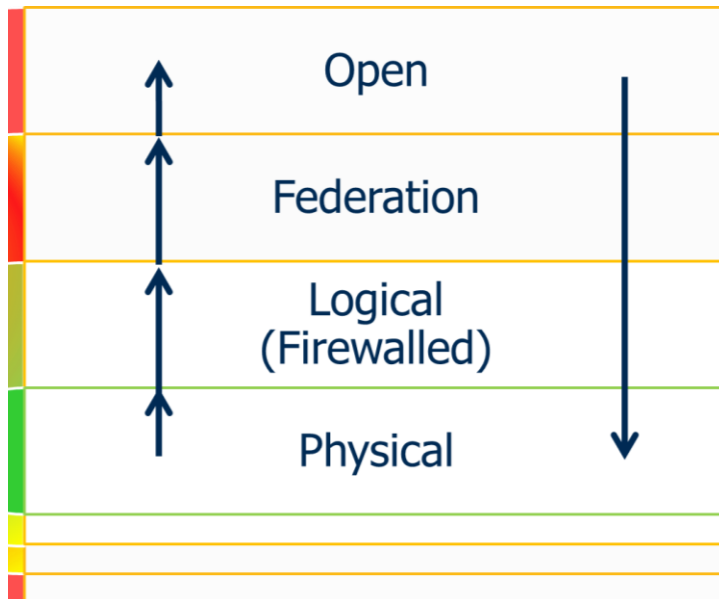
- ◆ What? – is the data
- ◆ Who? – has access
- ◆ Why? – do they need to know
- ◆ Where? – does it live and get accessed from
- ◆ When? – is it used
- ◆ How? – is it assigned and accessed



1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?

To Cloud or Not to Cloud

- ◆ Moves critical information to open or federated domains
- ◆ A good cloud is better than a weak local enterprise



1. What is the sensitive information in your organization?
2. Where is it?
3. Who has access to it?
4. Who you know and trust in your organization?
5. How do you insure against loss of sensitive information?

Wireless Problem Space



- ◆ Mobile phones limited by display size and computational limits (battery power)
 - Less user awareness of threat
- ◆ Wireless signals are visible to everyone
 - And could be interfered with by anyone
- ◆ Wireless networks eventually connect to wired networks
 - Subject to many of the same threats, plus many others
- ◆ Security involves both the networks and the applications that run on them
- ◆ Anyone can see anything you do on a mobile phone!

Social Engineering: the Insider Threat

- ◆ Start Simple: Use a hardware based keylogger
 - Provided physical access



- ◆ Install Keylogger
- ◆ Call IT for help – Have something fixed/installed
- ◆ Collect their credentials
- ◆ Enjoy!

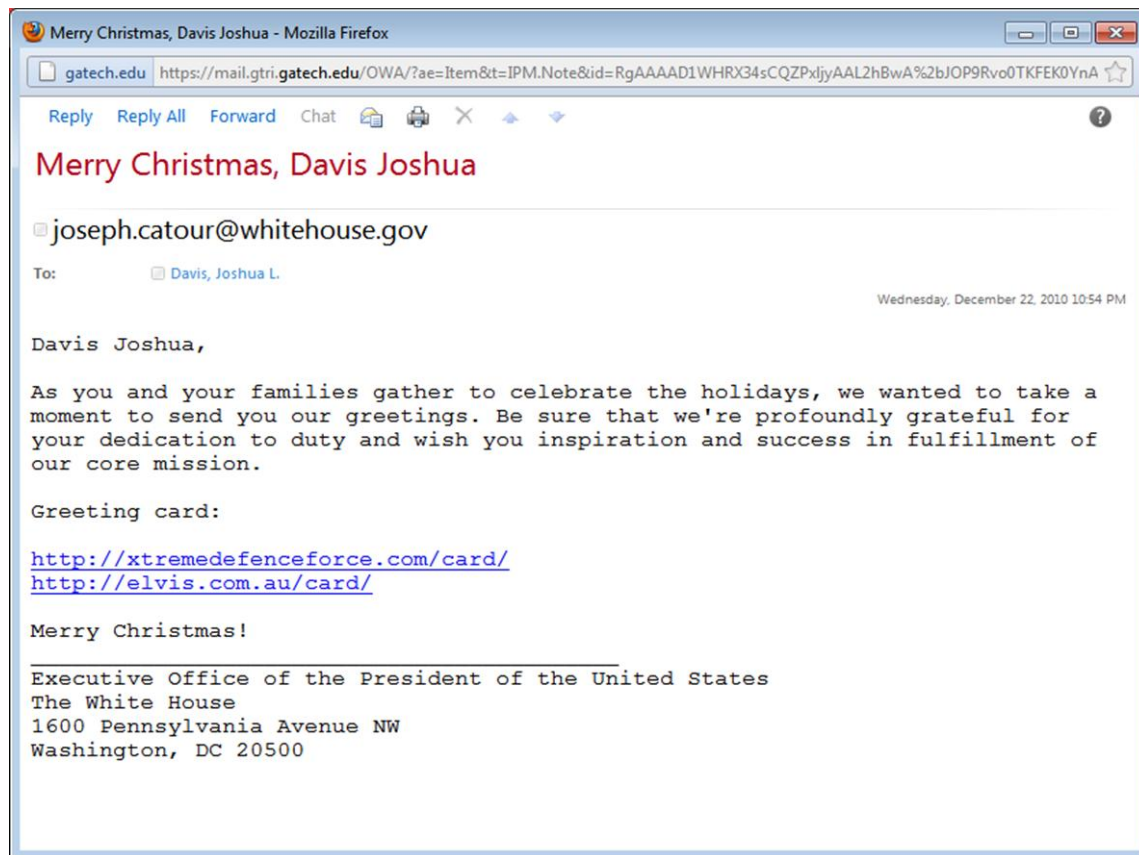
Username / Password

A screenshot of a Notepad window titled "LOG.TXT - Notepad". The window contains a log of keystrokes in a monospaced font. Two red arrows point from the text "Username / Password" above to the email address "jsmith29@mycompany.tld" and the password "BFG9000!!!!" in the log. The log text is as follows:

```
LOG.TXT - Notepad
File Edit Format View Help
[Alt]it.support[Shift]@mycompany.tld[Ent][Ent]
Support, Can you please install visual studio on my computer. It is imperative
that I get it installed as soon as possible. It is required for me to do my job
effectively.[Ent]
Thanks![Ent][Ent]
[Ct][Alt][DE]OFFICE-HQ\ADministrator[Tab]Qa139&nt8![Ent]
msdn.microsoft.com/subscriptions[Ent]
jsmith29@mycompany.tld[Tab]BFG9000!!!![Ent][Ent]
Cmd.exe
```

Phishing

- ◆ Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.



This is a Systems Problem

- ◆ No longer just an information technology issue
- ◆ Need to move from a vulnerability-centric model to a threat-centric model
- ◆ Need to move from a tool-centric perspective to a value-centric perspective
- ◆ Organizations must have a strategic cyber defense plan that drives their business approach
- ◆ The strategic plan must be threat-driven with targeted protection practices
- ◆ Protection practices center around information, not IT

The **Georgia Tech Information Security Center** and the **Georgia Tech Research Institute** provide a comprehensive set of academic, professional, and executive curricula from one of the leading security research and education programs in the world

GTCSS

Georgia Tech Cyber Security Summit **2011**

Presented by the **Georgia Tech Information Security Center (GTISC)**
and the **Georgia Tech Research Institute (GTRI)**

EMERGING
[CYBER THREATS]
REPORT **2012**